IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

TABITHA HANS-ARROYO, individually and on behalf of all others similarly situated, Plaintiff, v. WAWA, INC., Defendant.	CASE NO. **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

PLAINTIFF'S CLASS ACTION COMPLAINT

Benjamin F. Johns
Samantha E. Holbrook
Mark B. DeSanto
Andrew W. Ferich
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041
(610) 642-8500
bfj@chimicles.com
seh@chimicles.com
mbd@chimicles.com
awf@chimicles.com

Tina Wolfson
Bradley King
Henry Kelston
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, California 90024
Tel: (310) 474-9111
Fax: (310) 474-8585
twolfson@ahdootwolfson.com
bking@ahdootwolfson.com
hkelston@ahdootwolfson.com

Counsel for Plaintiff and the Putative Class

Plaintiff Tabitha Hans-Arroyo ("Plaintiff"), individually and on behalf of all others similarly situated, allege the following against Defendant Wawa, Inc. ("Wawa" or "Defendant") based on personal knowledge as to her own experience and upon information and belief on investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. Plaintiff brings this action, individually and on behalf of all other similarly situated individuals whose personal and non-public information, including credit card and debit card numbers, expiration dates, cardholder names, three or four-digit security codes (commonly referred to as "CVV" codes), and other payment card information (collectively, "Card Information") was compromised in a massive security breach of Wawa's payment processing servers and payment card environment that was publicly disclosed on December 19, 2019 (the "Data Breach").

2. As a result of the Data Breach, consumers who made purchases at Wawa's more than 850 convenience retail stores and gas pumps throughout Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, DC, have had their sensitive credit and debit Card Information exposed to hackers.

3. In an Open Letter from Wawa CEO Chris Gheysens to Our Customers (the "Open Letter") posted on Wawa's website on December 19, 2019, the very first sentence claims that "nothing is more important than honoring and protecting [the] trust" of its customers.[1] As evidenced by the occurrence of the Data Breach, this simply cannot be true.

[1] WAWA, *Open Letter from Wawa CEO Chris Gheysens to Our Customers* (Dec. 19, 2019), https://www.wawa.com/alerts/data-security (last accessed Dec. 20, 2019).

4. According to the Open Letter, Wawa's investigation to date has revealed that, at different points in time after March 4, 2019, malware began running on in-store payment processing systems at potentially all Wawa locations. Reportedly, this malware was present on most Wawa store systems by approximately April 22, 2019. Wawa's information security team did not identify this malware intrusion until December 10, 2019, and was unable to block and contain the malware until December 12.

5. The Open Letter confirmed that payment card information, including credit and debit card numbers, expiration dates, and cardholder names on payment cards used at potentially all Wawa in-store payment terminals and fuel dispensers was affected.

6. In addition to the Open Letter, Wawa's website contains a link to "FAQs" regarding the data breach, which explains, among other things, that in addition to in-store payment terminals and fuel dispensers, Wawa gift cards may also have been affected by the malware.[2]

7. Contrary to its Open Letter, Wawa clearly did not value customer data security and privacy enough to take adequate data security measures at its locations.

8. Aside from the Open Letter, upon information and belief, Wawa has yet to notify potentially impacted individuals.

9. As alleged herein, Wawa's failure to implement adequate data security measures to protect its customers' sensitive Card Information directly and proximately caused injuries to Plaintiff and class members.

10. The Data Breach was the inevitable result of Wawa's inadequate data security measures and cavalier approach to data security. Despite the well-publicized and ever-growing

[2] *See* FAQs (Dec. 19, 2019), available at https://www.wawa.com/alerts/data-security (last accessed Dec. 20, 2019).

threat of security breaches involving payment card networks and systems, and even though these types of data breaches were and are occurring frequently throughout the restaurant and retail industries, Wawa failed to ensure that it maintained adequate data security measures to protect customer Card Information from criminals.

11. As a direct and proximate result of Wawa's conduct and data security failures, a massive amount of customer information was stolen from Wawa and exposed to criminals. While Wawa has not confirmed the exact number of cards that were compromised, there are more than 850 locations on the East Coast which were all potentially affected.[3] Victims of the Data Breach have had their sensitive Card Information compromised, had their privacy rights violated, been exposed to the increased risk of fraud and identify theft, lost control over their personal and financial information, and otherwise have been injured.

12. Moreover, Plaintiff and class members have been and will be required to spend significant time associated with, among other things, closing out and opening new credit or debit card accounts, ordering replacement cards, obtaining fraud monitoring services, resolving loss of access to cash flow and credit lines, monitoring credit reports and accounts, purchasing identity theft insurance, and/or other losses resulting from the unauthorized use of their cards and accounts.

13. Wawa's offer to provide identity protection and credit monitoring service for one year at the credit monitoring website of Wawa's choice is too little too late, as Plaintiff and class members have already had their sensitive data exposed to criminals for up to nine months[4] and, as

[3] *See Beloved Regional Chain Wawa Data Breach Exposed 'Potentially All' Locations' Customer Data*, (Dec. 19, 2019), available at https://jezebel.com/beloved-regional-chain-wawa-data-breach-exposed-potenti-1840546342 (last accessed Dec. 20, 2019).

[4] *See* Resources for Our Customers, available at https://www.wawa.com/alerts/data-security (last accessed Dec. 20, 2019).

a result, will suffer increased vulnerability to fraudulent transactions and identity theft for many years into the future.

14. Plaintiff and class members seek to recover damages caused by Wawa's negligence, negligence *per se*, breach of contract, and violations of state consumer protection statutes. Additionally, Plaintiff seeks declaratory and injunctive relief as a result of the conduct of Wawa discussed herein.

PARTIES

A. Plaintiff Tabitha Hans-Arroyo

15. Plaintiff Tabitha Hans-Arroyo is an adult residing in Woodbury Heights, New Jersey. Ms. Hans-Arroyo used her Capital One credit card at various Wawa locations on a near-daily basis during the Data Breach window.

16. Early in the morning on December 24, 2019, Ms. Hans-Arroyo received an email from Capital One notifying her that a recent fraudulent purchase on Walmart.com in the amount of $2535.15 was declined due to a lack of available credit. Ms. Hans-Arroyo called Capital One to let them know that the transaction was fraudulent and unauthorized. Capital One directed Ms. Hans-Arroyo to a call center to confirm that her card information had been compromised. The call center representative confirmed that Ms. Hans-Arroyo's credit card had been compromised in the Wawa Data Breach. To date, Wawa has not provided direct notice of the Data Breach to Ms. Hans-Arroyo.

17. As a result, Capital One locked both Ms. Hans-Arroyo's credit card on December 24, 2019, the day before Christmas. Until Capital One issues Ms. Hans-Arroyo new card, she has no access to her credit card funds.

18. Prior to being victimized by the Wawa Data Breach, Ms. Hans-Arroyo's Capital One card had never been subjected to theft or fraud.

19. Had Ms. Hans-Arroyo known that Wawa would not adequately protect her Card Information and other sensitive information entrusted to it, she would not have made regular purchases at Wawa using her credit card.

20. As a result of Wawa's failure to adequately safeguard Plaintiff Hans-Arroyo's Card Information, she has been injured.

B. Defendant Wawa, Inc.

21. Defendant Wawa, Inc. maintains its headquarters at 260 West Baltimore Pike, Wawa, Pennsylvania 19063.

22. Wawa is a privately-held company that owns and operates over 850 convenient stores and gas stations located along the east coast in Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C. Reports indicate that Wawa stores serve roughly 800 million customers annually.[5]

23. With over $10 billion in annual revenue and approximately 34,000 employees, Wawa is one of the largest privately held corporations in the United States. According to Forbes, it ranks as the 25th largest private company in the country in 2019.[6]

JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million,

[5] Danya Henninger, *How Wawa makes money: $10 billion in sales and other fun facts*, BILLYPENN (May 27, 2018, 1:30 p.m.), available at https://billypenn.com/2018/05/27/how-wawa-makes-money-10-billion-in-sales-and-other-fun-facts/ (last accessed Dec. 20, 2019).
[6] *See America's Largest Private Companies*, FORBES, available at https://www.forbes.com/largest-private-companies/list/#tab:rank_search:wawa (last accessed Dec. 20, 2019).

exclusive of interest and costs, and is a class action in which some members of the class are citizens of states different than Wawa. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

25. This Court has personal jurisdiction over Wawa, because Wawa has sufficient minimum contacts with the state of Pennsylvania. Wawa maintains its headquarters in the Commonwealth of Pennsylvania and operates numerous Wawa locations and conducts substantial business within this judicial district. Wawa intentionally avails itself of the consumers and markets within the state of Pennsylvania through the promotion, marketing, and sale of its products and services. Thus, this Court has general personal jurisdiction over Wawa. Furthermore, Wawa directs its activities at residents of Pennsylvania on a constant and regular basis by way of, *inter alia*, its operation of hundreds of retail stores in Pennsylvania, and Plaintiff's and the class' claims arise out of Wawa's operation of retail stores in Pennsylvania; therefore, this Court also has specific personal jurisdiction over Wawa.

26. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because, as noted above, Wawa conducts substantial business in this district. A substantial part of the events and/or omissions giving rise to the claims occurred within this district.

FACTUAL ALLEGATIONS

A. The Wawa Data Breach

27. On December 19, 2019, Wawa posted "An Open Letter from Wawa CEO Chris Gheysens to Our Customers" on its website, which indicated that it had been made aware of a malware intrusion on Wawa's payment processing servers that compromised its payment card environment and customers' sensitive Card Information. The Open Letter provides the following, in pertinent part:

> Dear Wawa Customers,
>
> At Wawa, the people who come through our doors every day are not just customers, you are our friends and neighbors, and nothing is more important than honoring and protecting your trust. Today, I am very sorry to share with you that Wawa has experienced a data security incident. Our information security team discovered malware on Wawa payment processing servers on December 10, 2019, and contained it by December 12, 2019. This malware affected customer payment card information used at potentially all Wawa locations beginning at different points in time after March 4, 2019 and until it was contained. At this time, we believe this malware no longer poses a risk to Wawa customers using payment cards at Wawa, and this malware never posed a risk to our ATM cash machines.[7]

28. As confirmed by the Open Letter, Wawa believes the Data Breach occurred sometime on or after March 4, 2019, yet Wawa did not discover it until December 10, 2019, leaving customers' sensitive information exposed to criminals for nearly nine months.

29. The Open Letter also revealed that, while there were different timeframes for the Data Breach at Wawa's different locations, the malware affected most of its store systems. The Open Letter states:

> Based on our investigation to date, we understand that ***at different points in time*** after March 4, 2019, malware began running on in-store payment processing systems at potentially all Wawa locations. Although ***the dates may vary and some Wawa locations may not have been affected at all***, this malware was present on ***most store systems*** by approximately April 22, 2019. Our information security team identified this malware on December 10, 2019, and by December 12, 2019, they had blocked and contained this malware.[8]

30. In addition to the Open Letter, Wawa also issued a Press Release,[9] notifying customers of the data security incident:

---

[7] *See* Open Letter, *supra* n.1.
[8] *Id.* (emphasis added).
[9] *See* Press Release: *Wawa Notifies Customers of Data Security Incident* (Dec. 19, 2019), available at https://s3.amazonaws.com/wawa-kentico-prod/wawa/media/misc/wawa-data-security-incident-wire-release-12_19_2019.pdf (last accessed Dec. 20, 2019).

Contact: public.relations@wawa.com

Wawa Notifies Customers of Data Security Incident

Wawa, PA (December 19, 2019) – Wawa is notifying potentially impacted individuals about a data security incident that affected customer payment card information used at potentially all Wawa locations during a specific timeframe. Based on the investigation to date, the information is limited to payment card information, including debit and credit card numbers, expiration dates and cardholder names, but does not include PIN numbers or CVV2 numbers. The ATM cash machines in Wawa stores were not impacted by this incident. At this time, Wawa is not aware of any unauthorized use of any payment card information as a result of this incident.

Wawa's information security team discovered malware on Wawa payment processing servers on December 10, 2019, and contained it by December 12, 2019. After discovering this malware, Wawa immediately engaged a leading external forensics firm and notified law enforcement. Based on Wawa's forensic investigation, Wawa now understands that this malware began running at different points in time after March 4, 2019. Wawa took immediate steps after discovering this malware and believes it no longer poses a risk to customers.

"At Wawa, the people who come through our doors are not just customers, they are our friends and neighbors, and nothing is more important than honoring and protecting their trust," said Chris Gheysens, Wawa CEO. "Once we discovered this malware, we immediately took steps to contain it and launched a forensics investigation so that we could share meaningful information with our customers. I want to reassure anyone impacted they will not be responsible for fraudulent charges related to this incident. To all our friends and neighbors, I apologize deeply for this incident."

Wawa is supporting its customers by offering identity protection and credit monitoring services at no charge to them. Information about how to enroll can be found on the Wawa website below. Wawa has also established resources to answer customers' questions, including a dedicated call center that can be reached at 1-844-386-9559, Monday - Friday, between 9:00 am and 9:00 pm Eastern Time or Saturday and Sunday between 11:00 am and 8:00 pm, excluding holidays. Wawa has also posted information on its website, www.wawa.com, including a letter from Wawa's CEO and more details for impacted customers.

A detailed notice and open letter to customers from Wawa's CEO notifying potentially affected individuals about the incident is available at www.wawa.com/alerts/data-security

31. However, neither the Open Letter, Press Release, nor any statements issued by Wawa give any indication as to the *actual* magnitude of the Data Breach, including confirmation of the exact number of stores impacted or the actual number of customers and cards affected.

32. Although the Open Letter indicates Wawa also "notified law enforcement and payment card companies, and engaged a leading external forensics firm to support our response efforts,"[10] it is still unclear what such efforts involve, as Wawa has not disclosed exactly what was communicated to authorities.

B. Industry Standards and the Protection of Customer Card Information

33. It is well known in the retail industry that sensitive Card Information is valuable and frequently targeted by hackers. In a recent article, Business Insider noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers …. Many of them were caused by flaws in payment systems either online or in stores."[11]

34. One commentator in the data security industry noted as to a previous, unrelated data breach:

> POS-malware breaches happen in the US with alarming regularity, and businesses should be well aware that they need to not only protect their central networks but also need to account for physical locations as well. . . . Moving forward, financial institutions should consider implementing a system of two-factor authentication in conjunction with a passive biometric solutions in order to mitigate the entirely avoidable outcomes of security incidents such as this.[12]

35. Despite the known risk of point-of-sale (POS) malware intrusions and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Wawa failed to take reasonable steps to adequately protect its computer systems and payment card environment from being breached, and then failed to detect the Data Breach for many months.

---

[10] *Id*.

[11] Dennis Green and Mary Hanbury, *If you bought anything from these 11 companies in the last year, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 11:05 a.m.), available at https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last accessed Dec. 16, 2019).

[12] *Cyber Attack on Earl Enterprises (Planet Hollywood)*, isBuzznews (Apr. 1, 2019), available at https://www.informationsecuritybuzz.com/expert-comments/cyber-attack-on-earl-enterprises-planet-hollywood/ (last accessed Dec. 16, 2019).

36. Wawa is, and at all relevant times has been, aware that the Card Information it maintains as a result of purchases made at its locations is highly sensitive and could be used for nefarious purposes by third parties.

37. Wawa's explicit statements in its Privacy Policy make clear that Wawa recognized the importance of adequately safeguarding its customers' sensitive Card Information, yet Wawa failed to take the steps necessary to protect that sensitive data. On its website, Wawa's Privacy Policy provides the following:

> Wawa Official Privacy Policy
>
> Protecting your privacy is important to Wawa. This Wawa Privacy Policy ('Policy') describes how Wawa and its subsidiaries and affiliated companies collect, use, disclose and safeguard the personal information you provide on Wawa's websites, www.wawa.com and www.wawarewards.com, and through or in connection with our mobile apps or other software- and Internet-enabled programs and services sponsored by Wawa (the "Sites") as well as information collected when you visit our stores or otherwise communicate or interact with Wawa.[13]

38. The Privacy Policy goes on to explain the types of information collected and how Wawa may use such information.

39. Wawa is thus aware of the importance of safeguarding its customers' Card Information from the foreseeable consequences that would occur if its data security systems and computer servers were breached.

40. Financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure that consumers' valuable data is protected.

[13] *See* Wawa Official Privacy Policy (Effective Date: May 2019), available at https://www.wawa.com/privacy (last accessed Dec. 20, 2019).

41. The Payment Card Industry Data Security Standard ("PCI DSS") is a list of twelve information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted, and requires merchants like Wawa to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

42. The twelve requirements of the PCI DSS are: (1) Install and maintain a firewall configuration to protect cardholder data; (2) Do not use vendor-supplied defaults for system passwords and other security parameters; (3) Protect stored cardholder data; (4) Encrypt transmission of cardholder data across open, public networks; (5) Protect all systems against malware and regularly update anti-virus software or programs; (6) Develop and maintain secure systems and applications; (7) Restrict access to cardholder data by business need to know; (8) Identify and authenticate access to system components; (9) Restrict physical access to cardholder data; (10) Track and monitor all access to network resources and cardholder data; (11) Regularly test security systems and processes; (12) Maintain a policy that addresses information security for all personnel.[14]

43. Furthermore, PCI DSS sets forth detailed and comprehensive requirements that must be followed to meet each of the twelve mandates.

[14] PCI SECURITY STANDARDS COUNCIL, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard Version 3.2*, at 9 (May 2016), available at https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_2.pdf?agreement=true&time=1506536983345 (last accessed Dec. 20, 2019).

44. Wawa was, at all material times, fully aware of its data protection obligations in light of its participation in the payment card processing networks and its daily collection and transmission of thousands of sets of Card Information.

45. Because Wawa accepted payment cards containing sensitive financial information, it knew that its customers were entitled to and did in fact rely on it to keep that sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements.

46. Additionally, according to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45.

47. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

48. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly

assessing risks to computer systems, and implementing safeguards to control such risks.[15]

49. The FTC has issued orders against businesses that failed to employ reasonable measures to secure payment card data. These orders provide further guidance to businesses with regard to their data security obligations.

C. Wawa Disregarded Industry Standards for Customer Data Security

50. As noted above, Wawa should have been and, based upon its acknowledged use of encryption technology at certain locations, was aware of the need to have adequate data security systems in place.

51. Despite this, Wawa failed to upgrade and maintain its data security systems in a meaningful way in order prevent data breaches. Wawa's security flaws run afoul of industry best practices and standards. More specifically, the security practices in place at Wawa are in stark contrast and directly conflict with the PCI DSS core security standards.

52. Had Wawa properly maintained its information technology systems ("IT systems"), adequately protected them, and had adequate security safeguards in place, it could have prevented the Data Breach and/or could have promptly detected the Data Breach when it occurred.

53. As a result of industry warnings, awareness of industry best practices, the PCI DSS, and numerous well-documented restaurant and retail (and other) data breaches, Wawa was alerted to the risk associated with failing to ensure that its IT systems were adequately secured.

54. Wawa was not only aware of the threat of data breaches, generally, but was aware of the specific danger of malware infiltration. Malware has been used recently to infiltrate large retailers such as, *inter alia*, Target, GameStop, Chipotle, Jason's Deli, Whole Foods, Sally Beauty,

[15] FEDERAL TRADE COMMISSION, *Protecting Personal Information: A Guide for Business* (Nov. 2011), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed Dec. 20, 2019).

Neiman Marcus, Michaels Stores, Hy-Vee, and Supervalu. As a result, Wawa was aware that malware is a real threat and is a primary tool of infiltration used by hackers seeking to carry out payment card breaches.

55. In addition to the publicly announced data breaches described above (among many others), Wawa knew or should have known of additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted retailers to the threat of malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of malware, which was updated on August 27, 2014.[16]

56. Despite the fact that Wawa was on notice of the very real possibility of consumer data theft associated with its security practices and that Wawa knew or should have known about the elementary infirmities associated with its security systems, it still failed to make necessary changes to its security practices and protocols, and permitted the Data Breach to continue for approximately nine months.

57. Wawa, at all times relevant to this action, had a duty to Plaintiff and members of the class to: (a) properly secure Card Information submitted to or collected at Wawa's locations and on Wawa's internal networks; (b) encrypt Card Information using industry standard methods; (c) use available technology to defend its systems from known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiff and class members, which would naturally result from Card Information theft; and (e) promptly notify customers when Wawa became aware that customers' Card Information may have been compromised.

[16] *See* U.S. COMPUTER EMERGENCY READINESS TEAM, *Alert (TA14-212A): Backoff Point-of-Sale Malware* (July 31, 2014) (revised Sept. 30, 2016), https://www.us-cert.gov/ncas/alerts/TA14-212A (last accessed Dec. 20, 2019).

58. Wawa permitted customers' Card Information to be compromised by failing to take reasonable steps against a known threat.

59. In addition, leading up to the Data Breach, during the breach itself, and during the investigation that followed, Wawa failed to follow the guidelines set forth by the FTC.

60. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[17]

61. The Data Breach is particularly egregious and Wawa's data security failures are particularly alarming given that the breach went undetected for so long, exposing millions of customers' sensitive data to criminals for nearly nine months. Clearly, had Wawa utilized adequate data security and data breach precautions, the window of the Data Breach would have been significantly mitigated, and the level of impact significantly reduced (had the breach been permitted to occur at all).

62. With more than 850 Wawa locations potentially affected, and likely millions of sets of Card Data stolen, this clearly marks a highly successful outing for criminals and a large failure on Wawa's part as to data security.

63. Because payment card data breaches involving malware are so common, and given the high level of data security measures available to companies that take customer payment information in, like Wawa, there is no reason why Wawa could not have adequately protected its systems and servers from the Data Breach.

---

[17] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY (last accessed Dec. 20, 2019).

64. As a result of the Data Breach, Plaintiff and class members suffered actual fraud and losses resulting from the Data Breach, including: financial losses related to the purchases made at Wawa that Plaintiff and class members would not have made had they known of Wawa's negligent approach to cybersecurity; lost control of Card Data; unreimbursed losses relating to fraudulent charges; losses and fees relating to exceeding credit and debit card limits, balances, and bounced transactions; harm resulting from damaged credit scores and information; loss of time and money resolving fraudulent charges; loss of time and money monitoring accounts for fraudulent transactions, loss of time and money obtaining protections against future identity theft; loss of rewards points or airline mileage available on credit cards that consumers lost credit for as a result of having to use alternative forms of payment while awaiting replacement cards; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information.

65. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges occur and are discovered.

66. Furthermore, the Card Information stolen from Wawa's locations can be used to drain debit card-linked bank accounts, make "clone" credit cards, or to buy items on certain less-secure websites.

67. Recognizing the repercussions from its wrongful actions and inactions and the resulting Data Breach, Wawa claims it is now offering credit monitoring and identity protection at the credit monitoring bureau of its choice. However, this belated remedy does nothing to protect against the millions of customers who had their sensitive data exposed to criminals for nearly nine months, and does not ensure protection from fraud going forward. Furthermore, upon information and belief, to date Wawa has not offered to reimburse customers who have already paid for their

own fraud protection or credit monitoring services after learning of the data breach on or after December 12, 2019.

68. Wawa's failure to adequately protect its customers' Card Information has resulted in consumers having to undertake various tasks (e.g., obtaining credit monitoring, checking credit reports, monitoring accounts, etc.) that require time and effort and, for many of the credit and fraud protection services, payment of their own money. At the same time, Wawa is doing nothing to assist those affected by the Data Breach and has withheld important details about the Data Breach as it conducts its investigation. Instead, Wawa is putting the burden on the consumer to discover possible fraudulent transactions.

CLASS ALLEGATIONS

69. Plaintiff brings this action individually and on behalf of the following class ("the class") pursuant to Fed. R. Civ. P. 23:

> All persons who had their credit or debit card information compromised as a result of the Wawa Data Breach.

70. Excluded from the class are Wawa, its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change, or expand the definitions of the class based on discovery and further investigation.

71. **Numerosity**: While the precise number of class members has not yet been determined, members of the class are so numerous that their individual joinder is impracticable, as the proposed class includes many geographically dispersed class members. Upon information and belief, the Data Breach affected thousands, if not millions, of Wawa customers across the United States.

72. **Typicality**: Plaintiff's claims are typical of class members' claims. Plaintiff and all class members were injured through Wawa's uniform misconduct. The same event and conduct

that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other class member because Plaintiff and each class member had their sensitive data and Card Information compromised in the same way by the same conduct by Wawa.

73. **Adequacy**: Plaintiff is an adequate representative of the class because Plaintiff's interests do not conflict with the interests of the class that they seek to represent; Plaintiff has retained counsel that are competent and highly experienced in class action litigation, including data breach cases in particular; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the class will be fairly and adequately protected by Plaintiff and her counsel.

74. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the class members. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for class members individually to effectively redress Wawa's wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

75. **Existence and Predominance of Common Questions of Fact and Law**: Common questions of law and fact exist as to Plaintiff and all class members. These questions predominate over the questions affecting individual class members. These common legal and

factual questions include, but are not limited to, the following:

(a) whether Wawa engaged in the wrongful conduct alleged herein;

(b) whether Wawa owed duties to Plaintiff and members of the class to protect their Card Information and to provide timely and accurate notice of the Data Breach to Plaintiff and the class, and whether it breached these duties;

(c) whether Wawa violated federal and state laws as a result of the Data Breach;

(d) whether Wawa knew or should have known that its computer and network systems were vulnerable to attacks from hackers and cyber-criminals;

(e) whether Wawa's conduct was the proximate cause of the breach of its computer and network systems resulting in the theft of customers' Card Information;

(f) whether Wawa wrongfully failed to inform Plaintiff and members of the class that it did not maintain computer software and other security procedures and precautions sufficient to reasonably safeguard consumers' sensitive financial and personal data;

(g) whether Wawa failed to inform Plaintiff and the class of the Data Breach in a timely and accurate manner;

(h) whether Wawa has taken adequate preventive and precautionary measures to ensure Plaintiff and class members will not experience further harm;

(i) whether Wawa violated the New Jersey Consumer Fraud Act;

(j) whether Plaintiff and members of the class suffered injury as a proximate result of Wawa's conduct or failure to act; and

(k) whether Plaintiff and the class are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiff and the class.

76. Wawa has acted or refused to act on grounds generally applicable to Plaintiff and the other members of the class, thereby making appropriate final injunctive relief and declaratory relief with respect to the class as a whole.

77. Given that Wawa has engaged in a common course of conduct as to Plaintiff and the class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

78. The class is defined in terms of objective characteristics and common transactional

facts; namely, the exposure of sensitive Card Information to cyber criminals due to Wawa's failure to protect this information, adequately warn the class that it lacked adequate data security measures, and failure to adequately warn that it was breached. Class membership will be readily ascertainable from Wawa's business records, and/or from records of third parties.

79. Plaintiff reserves the right to revise the above class definitions and any of the averments of fact herein based on facts adduced in discovery.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

80. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

81. Wawa collected Card Information from Plaintiff and class members in exchange for its sale of food and other services at its impacted locations.

82. Wawa owed a duty to Plaintiff and the class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their financial and personal information in Wawa's possession from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Wawa's networks and data security systems to ensure that Plaintiff's and class members' financial and personal information in Wawa's possession was adequately protected in the process of collection and following collection while stored on Wawa's systems.

83. Wawa further owed a duty to Plaintiff and class members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

84. Wawa owed a duty to Plaintiff and class members to provide security consistent with industry standards and requirements and to ensure that its computer systems and networks—and the personnel responsible for them—adequately protected the financial and personal information of Plaintiff and class members whose confidential data Wawa obtained and maintained.

85. Wawa knew, or should have known, of the risks inherent in collecting and storing Plaintiff's and class members' financial and personal information and the critical importance of providing adequate security for that information.

86. Wawa's conduct created a foreseeable risk of harm to Plaintiff and class members. This conduct included but was not limited to Wawa's failure to take the steps and opportunities to prevent and stop the Data Breach as described herein. Wawa's conduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the financial and personal information of Plaintiff and class members.

87. Wawa knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Wawa knew or should have known that hackers would attempt or were attempting to access the personal financial information in databases such as Wawa's.

88. Wawa breached the duties it owed to Plaintiff and members of the class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the medical, financial, and personal information of Plaintiff and members of the class, as identified above. This breach was a proximate cause of injuries and damages suffered by Plaintiff and class members.

89. As a direct and proximate result of Wawa's negligent conduct, Plaintiff and class members have been injured and are entitled to damages in an amount to be proven at trial.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

90. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

91. Pursuant to the FTC Act, 15 U.S.C. § 45, Wawa had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and class members' personal information.

92. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Wawa, of failing to use reasonable measures to protect Card Information. The FTC publications and orders described above also form part of the basis of Wawa's duty to protect Plaintiff's and class members' sensitive information.

93. Wawa violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Card Information and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Wawa's conduct was particularly unreasonable given the nature and amount of Card Information it collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to consumers and financial institutions.

94. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and

avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the class.

95. Wawa had a duty to Plaintiff and class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and class members' personal information.

96. Wawa breached its duties to Plaintiff and class members under the FTC Act (and similar state statutes), by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and class members' financial and personal information.

97. Wawa's violation of Section 5 of the FTC Act (and similar state statutes) and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

98. But for Wawa's wrongful and negligent breach of its duties owed to Plaintiff and class members, they would not have been injured.

99. The injury and harm suffered by Plaintiff and class members was the reasonably foreseeable result of Wawa's breach of its duties. Wawa knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and class members to suffer the foreseeable harms associated with the exposure of their Card Information.

100. Had Plaintiff and class members known that Wawa did and does not adequately protect customer Card Information, they would not have made purchases at Wawa's locations.

101. As a direct and proximate result of Wawa's negligence *per se*, Plaintiff and class members have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the purchases made at Wawa that Plaintiff and class members would not have made had they known

of Wawa's careless approach to cyber security; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Card Information, entitling them to damages in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

102. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

103. Plaintiff and class members who made purchases at Wawa's locations during the period in which the Data Breach occurred had implied contracts with Wawa.

104. Specifically, Plaintiff and class members paid money to Wawa and, in connection with those transactions, provided Wawa with their Card Information. In exchange, Wawa agreed, among other things: (1) to provide food, gasoline, and food services to Plaintiff and class members at its various locations; (2) to take reasonable measures to protect the security and confidentiality of Plaintiff's and class members' Card Information; and (3) to protect Plaintiff's and class members' personal information in compliance with federal and state laws and regulations and industry standards.

105. Protection of personal information is a material term of the implied contracts between Plaintiff and class members, on the one hand, and Wawa, on the other hand. Indeed, as set forth, *supra*, Wawa recognized the importance of data security and privacy of customers' sensitive financial information in the privacy policy. Had Plaintiff and class members known that

Wawa would not adequately protect customer Card Information, they would not have made purchases at Wawa's locations.

106. Wawa did not satisfy its promises and obligations to Plaintiff and class members under the implied contracts because it did not take reasonable measures to keep their personal information secure and confidential and did not comply with the applicable laws, regulations, and industry standards.

107. Wawa materially breached its implied contracts with Plaintiff and class members by failing to implement adequate payment card and Card Information security measures.

108. Plaintiff and class members fully performed their obligations under their implied contracts with Wawa.

109. Wawa's failure to satisfy its obligations led directly to the successful intrusion of Wawa's computer servers and stored Card Information and led directly to unauthorized parties access and exfiltration of Plaintiff's and class members' Card Information.

110. Wawa breached these implied contracts as a result of its failure to implement security measures.

111. Also, as a result of Wawa's failure to implement the security measures, Plaintiff and class members have suffered actual damages resulting from the theft of their personal information and remain at imminent risk of suffering additional damages in the future.

112. Accordingly, Plaintiff and class members have been injured as a proximate result of Wawa's breaches of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
BREACH OF CONTRACTS TO WHICH PLAINTIFF AND CLASS MEMBERS WERE INTENDED THIRD-PARTY BENEFICIARIES
(On Behalf of Plaintiff and the Class)

113. Plaintiff realleges and incorporates all foregoing substantive allegations as if fully set forth herein.

114. Upon information and belief, Plaintiff and class members are intended third-party beneficiaries of contracts entered into between Wawa and various entities including, without limitation, (i) contracts between Wawa and its customers to process credit card and/or debit card transactions, (ii) contracts between Wawa and Visa and/or MasterCard (including their operating regulations), and (iii) contracts between Wawa and the acquiring banks that accept and process payment card transactions at Wawa's locations.

115. Upon further information and belief, these contracts and regulations require, *inter alia*, that Wawa take appropriate steps to safeguard the sensitive financial information of Wawa's customers, like Plaintiff and class members.

116. Plaintiff and the class members are intended third party beneficiaries of these contracts and regulations. Under the circumstances, recognition of a right to performance is appropriate to effectuate the intentions of the parties to these contracts. One or more of the parties to these contracts intended to give Plaintiff and the class members the benefit of the performance promised in the contracts.

117. Wawa breached these agreements, which directly and/or proximately caused Plaintiff and the class members to suffer substantial damages.

118. Upon further information and belief, Wawa saved (or avoided spending) a substantial sum of money by knowingly failing to comply with its contractual obligations, and continues to do so.

119. Accordingly, Plaintiff and class members who have been injured are entitled to damages, restitution, and other relief in an amount to be proven at trial.

COUNT V
VIOLATION OF THE NEW JERSEY CONSUMER FRAUD ACT, N.J. STAT. ANN. §56:8-2, *et seq.*
(On Behalf of Plaintiff and the Class)

120. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

121. Plaintiff Hans-Arroyo and members Class are consumers who used their credit or debit cards to purchase convenient store items and gasoline products for personal, family and household purposes from Wawa locations in New Jersey.

122. Wawa engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the sale of "merchandise" to consumers, as defined by N.J. STAT. ANN. § 56:8-1.

123. Wawa is engaged in, and its acts and omissions affect, trade and commerce. Wawa's relevant acts, practices and omissions complained of in this action were done in the course of Wawa's business of marketing, offering for sale and selling food products, gasoline, goods and services throughout the state of New Jersey and the Eastern United States.

124. The New Jersey Consumer Fraud Act ("NJCFA"), N.J. STAT. ANN. § 56:8-2, *et seq.*, prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New Jersey.

125. In the conduct of its business, trade, and commerce, and in the sale of food products, gasoline, goods or services to consumers in the state of New Jersey, Wawa collected and stored highly personal and private information, including sensitive financial information of Wawa's customers, like Plaintiff and members of the Class.

126. Wawa knew or should have known that its computer systems and data security practices were inadequate to safeguard the sensitive financial information of the Class and that the risk of a data breach was highly likely and/or that the risk of the data breach being more extensive than originally disclosed was highly likely.

127. Wawa should have disclosed this information regarding its computer systems and data security practices because Wawa was in a superior position to know the true facts related to the security vulnerability, and members of the Class could not reasonably be expected to learn or discover the true facts.

128. As alleged herein, Wawa engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the sale of food products, gasoline products, goods or services to consumers in the state of New Jersey, in violation of the NJCFA, including but not limited to:

(a) Failing to adequate secure the sensitive financial information of members of the Class;

(b) Failing to maintain adequate computer systems and data security practices to safeguard customers' personal and financial information;

(c) Misrepresenting the material fact that Wawa would maintain adequate data privacy and security practices and procedures to safeguard customer's sensitive financial information from unauthorized disclosure, release, data breaches, and theft;

(d) Misrepresenting the material fact that Wawa did and would comply with the requirements of relevant federal and state laws and industry standards pertaining to the privacy and security of the sensitive financial information of members of the Class;

(e) Knowingly omitting, suppressing, and concealing the material fact that Wawa's computer systems and data security practices were inadequate to safeguard customers' personal and financial data from theft, with the intent that others rely upon the omission, suppression, and concealment;

(f) Failing to disclose in a timely and accurate manner to the Class the material fact of the nature and extent of the Data Breach; and

(g) Continuing to accept credit and debit card payments and storage of other personal information after Wawa knew or should have known of the data breach and before it allegedly remedied the breach.

129. By engaging in the conduct alleged above, Wawa has violated the NJCFA by, *inter alia*:

(a) Omitting material facts regarding the goods and services sold;

(b) Omitting material facts regarding the financial transactions, particularly the security thereof, between Wawa and its customers for the purchase of food products, gasoline, goods and services;

(c) Misrepresenting material facts in the furnishing or sale of food products, gasoline, goods and services;

(d) Engaging in conduct that is likely to mislead consumers acting reasonably under the circumstances;

(e) Engaging in conduct which creates a likelihood of confusion or of misunderstanding;

(f) Engaging in conduct that is immoral, unethical, oppressive and unscrupulous;

(g) Unfair practices that caused or were likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers; and/or

(h) Other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial.

130. Wawa's actions engaging in the conduct above were negligent, knowing and willful and/or wanton and reckless with respect to the rights of the Class.

131. As a direct and proximate result of Wawa's violation of the NJCFA, members of the Class have suffered ascertainable losses of moneys and actual damages including, *inter alia*:

(a) unauthorized charges on their debit and credit card accounts;

(b) theft of their personal and financial information by criminals;

(c) costs associated with the detection and prevention of identity theft;

(d) costs associated with the unauthorized use of their financial accounts;

(e) loss and use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations;

(f) costs and lost time associated with handling the administrative consequences of the data breach, including identifying, disputing and seeking reimbursement for fraudulent charges, canceling and activating payment cards, and shopping for credit monitoring and identity theft protection;

(g) impending injury flowing from potential fraud and identity theft posed by their credit card and personal information being placed in the hands of criminals and already being misused;

(h) impairment to their credit scores and ability to borrow and/or obtain credit; and

(i) the continued risk to their personal information, which has been accessible to criminals for over nine months and which remains on Wawa's insufficiently secured computer systems.

132. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Wawa alleged herein, the Class seeks relief under N.J. STAT. ANN. § 56:8-19, including, but not limited to, actual damages, treble damages, injunctive relief, and attorneys' fees and costs.

133. Pursuant to N.J. STAT. ANN. § 56:8-20, this Complaint will be served upon the New Jersey Attorney General.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

134. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

135. This claim is plead in the alternative to the above implied contract claim.

136. Plaintiff and class members conferred a monetary benefit upon Wawa in the form of monies paid for the purchase of food and food-related services at its locations.

137. Wawa appreciated or had knowledge of the benefits conferred upon them by Plaintiff and class members. Wawa also benefited from the receipt of Plaintiff's and class members' Card Information, as this was utilized by Wawa to facilitate payment to it.

138. The monies Plaintiff and class members paid to Wawa were supposed to be used by Wawa, in part, to pay for adequate data privacy infrastructure, practices, and procedures.

139. As a result of Wawa's conduct, Plaintiff and class members suffered actual damages in an amount equal to the difference in value between their purchases made with adequate data privacy and security practices and procedures that Plaintiff and class members paid for, and those purchases without adequate data privacy and security practices and procedures that they received.

140. Under principals of equity and good conscience, Wawa should not be permitted to retain the money belonging to Plaintiff and class members because Wawa failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

141. Wawa should be compelled to disgorge into a common fund for the benefit of Plaintiff and class members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, on behalf of herself and the class, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23(a) and (b), and, pursuant to Fed. R. Civ. P. 23(g), appoint Plaintiff as class representatives and their counsel as class counsel.

B. Award Plaintiff and the class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement.

C. Award Plaintiff and the class equitable, injunctive, and declaratory relief as may be appropriate. Plaintiff, on behalf of the class, seeks appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information, extend credit monitoring services and similar services to protect against all types of identity theft, including card theft and fraudulent card charges, and to provide elevated credit monitoring services to minor and elderly class members who are more susceptible to fraud and identity theft.

D. Award Plaintiff and the class pre-judgment and post-judgment interest to the maximum extent allowable.

E. Award Plaintiff and the class reasonable attorneys' fees and costs as allowable.

F. Award Plaintiff and the class such other favorable relief as allowable under law or at equity.

Dated: December 26, 2019

Respectfully submitted,

/s/ Benjamin F. Johns

Benjamin F. Johns
Samantha E. Holbrook
Mark B. DeSanto
Andrew W. Ferich
CHIMICLES SCHWARTZ KRINER & DONALDSON-SMITH LLP
One Haverford Centre
361 Lancaster Avenue
Haverford, PA 19041

(610) 642-8500
bfj@chimicles.com
seh@chimicles.com
mbd@chimicles.com
awf@chimicles.com

Tina Wolfson
Bradley King
Henry Kelston
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, California 90024
Tel: (310) 474-9111
Fax: (310) 474-8585
twolfson@ahdootwolfson.com
bking@ahdootwolfson.com
hkelston@ahdootwolfson.com

Attorneys for Plaintiff